STRATEGY RESEARCH PROJECT

PROTECTING THE UNITED STATES AGAINST INFORMATION WARFARE

BY

LIEUTENANT COLONEL GARY BRAND
United States Air Force

USAWC CLASS OF 2000

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

Protecting the United States Against Information Warfare

by

Lt Col Gary Brand
United States Air Force

Colonel Nate Bard
Project Advisor

U.S. Army War College
Carlisle Barracks, Pennsylvania 17013

ABSTRACT

AUTHOR: Lt Col Gary Brand

TITLE: Protecting the United States Against Information Warfare

FORMAT: Strategy Research Project

DATE: 01 April 2000 PAGES: 38 CLASSIFICATION: Unclassified

The United States' reliance on computers and the Internet for everything, from banking to military command and control, has made the nation's information infrastructure highly vulnerable to infiltration and sabotage from a multitude of threats. This vulnerability is the "Achilles Heel" of U.S. global power and will be a major security challenge for the 21st Century. If the United States does not improve its ability to defend against information attacks, it may fall victim to a new and more destructive type of war, "Infowar." Although the government has taken the lead to protect its information infrastructure through several initiatives, there must be cooperative efforts between the government, industry, and private agencies working together as a team to protect this critical "Center of Gravity." For the United States to adequately protect its information infrastructure against a myriad of threats, it must identify its vulnerabilities and put "teeth" into its defensive information warfare policy.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

Invincibility depends on one's self; the enemy's vulnerability on him.

— Sun Tzu

If we are to continue to enjoy the benefits of the Information Age, preserve our security, and safeguard our economic well-being, we must protect our critical computer-controlled systems from attack.

— President William J. Clinton

PROTECTING THE UNITED STATES AGAINST INFORMATION WARFARE

The United States is now embarking on a new and potentially more destructive kind of war – "The Infowar." This is war fought by using computers and networks devoid of physical boundaries and comprising many threats to our critical information infrastructure. Every day in America there are thousands of unauthorized attempts to gain access to key government and industry networks, defense facilities, government agencies and civilian telephone and transportation systems.[1] All one has to do is pick up a newspaper and read the headlines such as, "Bank Losses Put at Millions in Computer Break-in" or "Hackers Disrupt Telephone Service,"[2] to realize that the United States needs a cooperative effort of the government, private industry and citizens to combat this menace to our way of life.

DEPENDENCE ON INFORMATION NETWORKS

The predominantly privately owned and operated National Information Infrastructure (NII) is what many consider the "Achilles Heel" of the nation in our Infowar fight. The NII was originally designed to be a system of high-speed telecommunications networks, databases, and advanced computer systems that make electronic information widely available and accessible.[3] The NII was designed and built for the private sector, but the government is also a significant user of the NII. In fact, 95 percent of DoD's unclassified data traffic flows over the nation's information infrastructure.[4] The nation now depends on interlinked information systems to conduct business. Today there are few entities that don't use the nation's information infrastructure in some capacity. Manufacturers, transportation providers, financial & banking institutions, federal, state, and local government, the military, and even private citizens "surfing" the web or sending e-mail, all use the NII.

There are many reasons why the NII has grown over the years. Producers and suppliers can use electronic links to lower costs by reducing inventories.[5] It has also been a profitable and more reliable means of transferring information. As late as ten years ago, a company would have to send a letter via Federal Express or use slower mail service. If an immediate transmission of the letter was necessary, the company would have to rely on a fax machine. Today, it could be as simple as e-mailing the information or posting it on a company's web site for download. E-commerce has grown at a tremendous rate as a result of the NII. From 1995 to 1999, on-line dollar growth increased from $450 Million to $6.1 Billion.[6] Today, you see many ads dealing with on-line trading of stocks. Ten years ago, that would have been

unthinkable. However, it is this changing of the information paradigm that has increased the NII vulnerability to attack. It is the disruption or intrusion of the NII by several potential protagonists that causes the most concern and puts the National Information Infrastructure at risk.

POTENTIAL CYBERATTACK PROTAGONISTS

The threat spectrum is composed of several different types of adversaries. They range from nation-state actors to recreational hackers. Each adversary has a motive for conducting cyberattacks against the United States.

NATION-STATES

On the high end of the threat spectrum there are several nations developing information warfare capabilities against the United States. These nation-states have three main objectives for infiltrating the United States' critical infrastructures: assist government-sponsored companies in acquiring an advantage over U.S. competitors; damage the economic stability of our nation by targeting our financial or industrial resources; or damage our national security by conducting military or intelligence operations.[7] China and other countries have already begun to focus on the United States' computer network as a target for information attacks in an attempt to cripple the U.S. information flow capability.[8]

At least five other nations (Syria, Iran, India, Pakistan and Israel) have active groups, paid by their governments, trying to formulate tools and procedures to cause computer terrorism in U.S. corporations.[9] In fact, today, over 60 percent of university degrees in Computer Science are given to students from developing countries, with a vast majority of those students coming from Islamic countries.[10]

CRIMINALS

The potential use of cyberattacks by organized crime groups, both domestic and international, is an immediate and increasing concern for the United States. Over the past five years, more than 72 percent of United States corporations found an increased security threat to their data.[11] A 1999 FBI survey revealed that from 1997 to 1999, computer crimes cost United States' corporations over $360 Million.[12]

Criminals are exploiting high technology for a variety of purposes, not the least of which is financial gain. The biggest targets appear to be credit card companies, telephone companies and financial institutions. For example, in 1994, there was an attack against Citibank's computers by a Russian based organized crime ring which resulted in a theft of over $12 Million.[13]

HACKERS

The majority of computer intrusions and disruptions to the nation's computer system come from hackers. At one time, hackers were characterized as computer-savvy teenagers and over-zealous programmers who harmlessly infiltrated networks and computers to prove their computer skills, and

thought of hacking into government computer networks as a game. They regarded these infiltrations as their civic responsibility to uncover security flaws.

Recently, hackers have begun to infiltrate computer systems for profit and many have become "hacktivists" using their hacking skills to deface government web pages or render sites unusable in order to send a message of revenge or protest. Examples of some of the targeted sites have been; The White House, Congress, DoD, Federal Agencies, and even the FBI. Their ability to cause significant damage is becoming more and more viable and could get increasingly more dangerous.

TERRORISTS

Terrorists in the past have sought to conduct violent acts against non-combatant targets with the intent to influence an audience. Traditionally, terrorism is defined as the systematic use of violence as a means to intimidate or coerce societies or governments. Typically, this has occurred through bombings or other attacks on targets with high profiles, or that raise significant media attention, or that symbolize the government or ideology to which the terrorist organization is opposed. However, the opportunities afforded by information warfare techniques have now provided terrorists greater tools to inflict fear into a civilian population or wreak havoc throughout targeted institutions. In his book, War and Anti-war, Toffler believed it was now possible for a Hindu fanatic in Hyderabad or a Muslim fanatic in Madras or even a deranged "nerd' in Denver to cause immense damage to people, countries, and even armies 10,000 miles away. A report of the National Research Council revealed that, "Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."[14]

Recently, a top Japanese cyberterrorism and crime expert, Raisuke Miyawaki, predicted that it is "only a matter of time" before all nations experience the first cyberattack on a worldwide scale. He also called cyberterrorism one of the two top post-Cold War problems the world faces, with the other being organized crime.[15]

INSIDERS

Insiders may be the greatest threat to our critical information infrastructure. It is the insider who is likely to have the best understanding of an organization's culture and the greatest knowledge about the operations of an infrastructure and its supporting systems.[16] At least 70 percent of intrusions come from inside an organization.[17] The insider threats can include disgruntled workers, paid informants, compromised or coerced employees, former employees, and business associates motivated to plan and conduct attacks for reasons such as revenge, financial gain, and fear.[18] Gary Hayward and Stewart Personick in their article, "Protecting the Infrastructures of the Information Age," suggest through the following "fictional" scenario, how an insider with the right access could create havoc and threaten the nation's information infrastructure.

Kathy was a bright computer-science graduate who worked at a major software firm whose applications were used by tens of millions of individuals and corporations worldwide. Within a few years,

Kathy gained a position of considerable responsibility in the company's software configuration-management operation.[19] Unfortunately the company was unaware that Kathy was also a member of a political group that was ready to make its agenda known to the world. Kathy took the opportunity to use her access privileges to plant a piece of sophisticated, malicious code in the latest release of her firm's most popular software application which, when loaded on computers, created havoc worldwide.[20] This scenario of a "trusted user" unfortunately is not too far fetched and could happen any day.

In summary, there is no shortage of potential threats to the United States. They can be foreign or domestic, internal or external, state-sponsored or a single rogue element, terrorist, insiders, disgruntled employees or hackers. Unfortunately, as technology has advanced over the past two decades, so have the tools and techniques of those who attempt to break into systems. Figure 2 shows how the technical knowledge required by an attacker decreases, as the sophistication of the tools and techniques increases.[21]

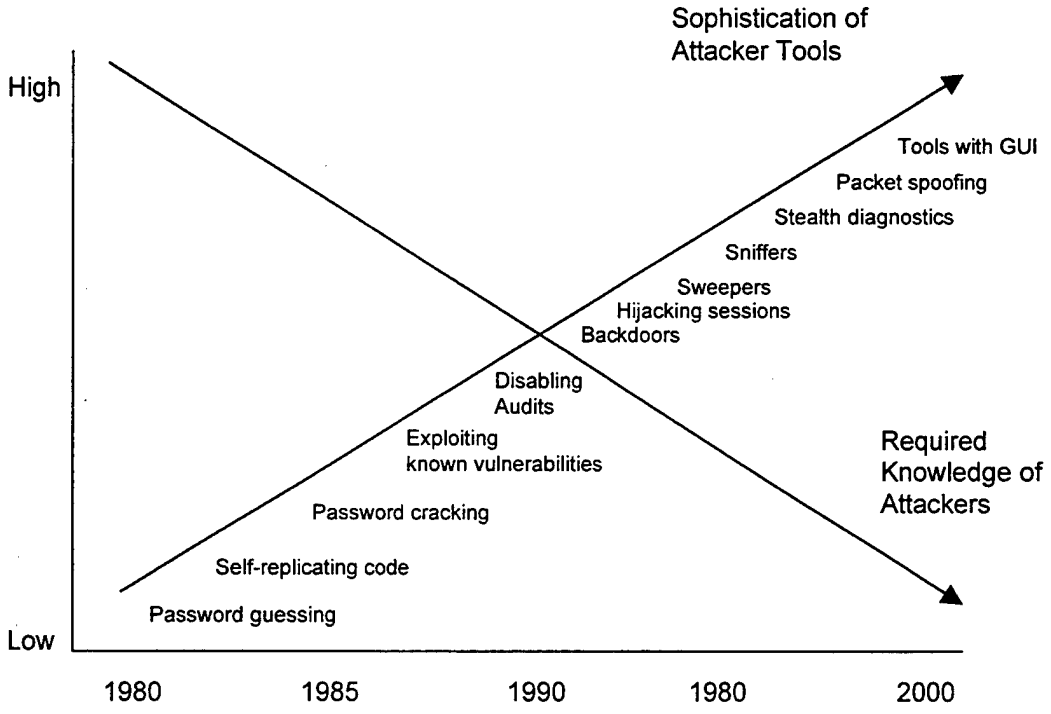


FIGURE 1. ATTACKERS REQUIRE LESS KNOWLEDGE AS TOOL SOPHISTICATION INCREASES

NATION UNDER SIEGE

Infowar has already begun to take place against the nation's information infrastructure. No one is immune from computer attack. The threat is real. Consider the following incidents of possible cyberattacks against three different sectors as cited in President Clinton's National Plan for Information Systems Protection:

1) "Two of America's largest cities have their 911 service disrupted, causing confusion, slow response, and potentially, needless deaths."[22]

2) "Widespread intrusions into Army, Navy, Air Force, and DoD logistics and support computer systems are discovered during the middle of our February 1998 confrontation with Iraq. There is no clear idea where the intrusions were coming from, how long they had been occurring, or what information had been removed or compromised."[23]

3) "A new computer virus moves rapidly across the Internet, overloading systems with superfluous e-mails and shutting down major portions of corporate and government systems."[24]

The Defense Information Systems Agency (DISA) estimates that DoD is attacked about 250,000 times per year in which only 1 in 500 attacks are detected and reported.[25] In the civilian sector, Figure 2 illustrates known computer intrusions monitored by The Computer Emergency Response Team (CERT) which shows a dramatic increase of computer intrusions from six in 1988 to 8,268 in 1999.[26]

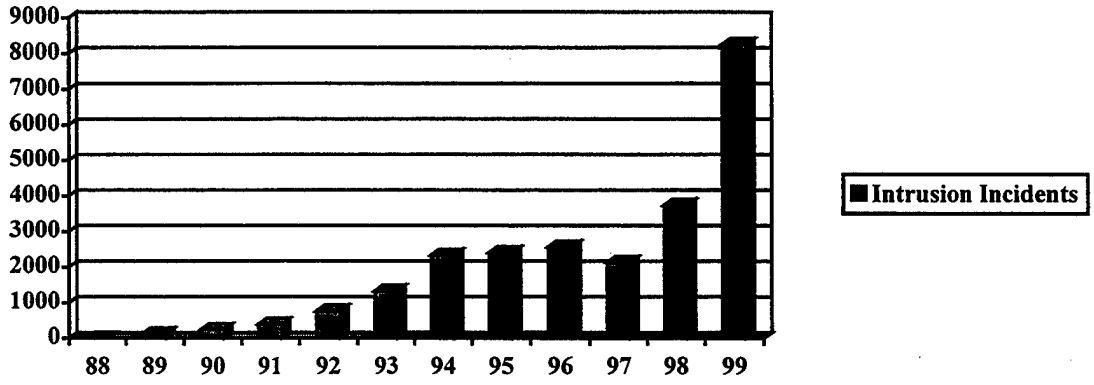


FIGURE 2. CERT TRACKED COMPUTER INTRUSIONS

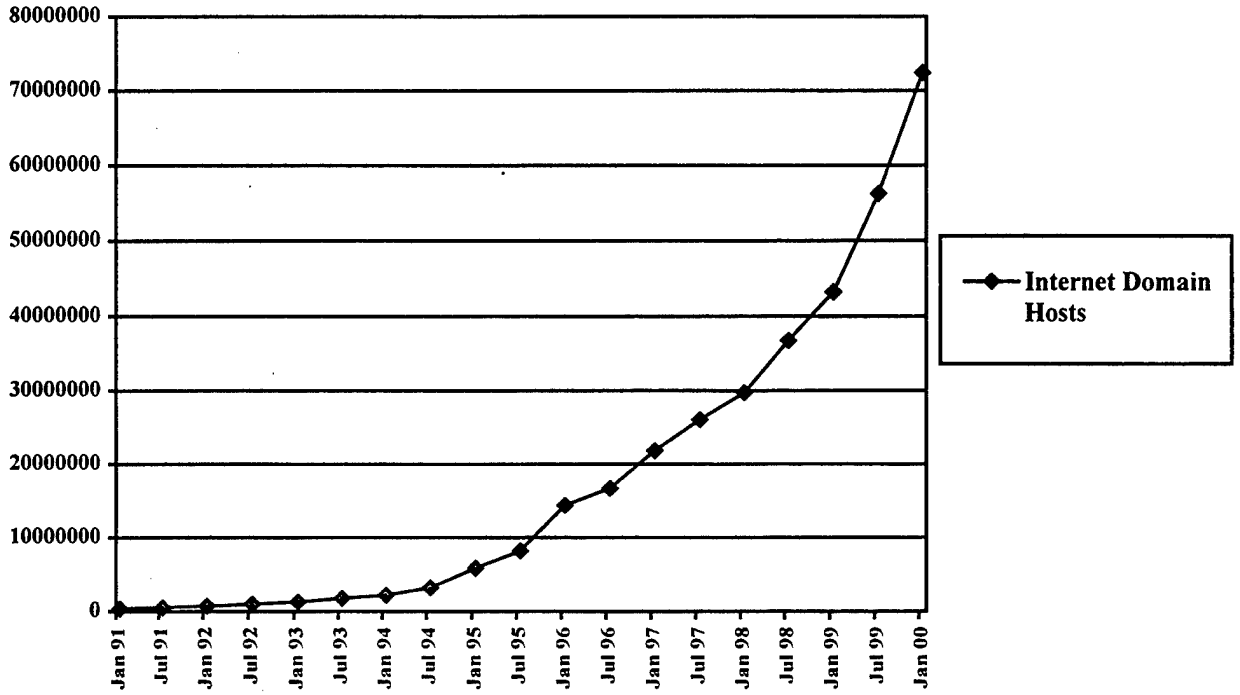
The cost of these attacks against the private sector reached over $123 Million in 1999.[27] The FBI's caseload for computer hacking and network intrusions has doubled each of the last two years.[28] A recent survey of over 520 U.S. corporations, government agencies, financial institutions and universities conducted by the Computer Security Institute revealed that 64 percent suffered an intrusion or other unauthorized use of computer systems, 25 percent reported denial of service attacks, 24 percent reported system penetration from the outside, 18 percent reported theft of proprietary information, 14 percent reported sabotage of data or networks and 72 percent suffered financial losses due to computer security breaches, including computer viruses.[29]

The defense is only as strong as its weakest link, and in this case, the most likely weak link in the information infrastructure is the increased reliance on the Internet and the relatively weak network security in the civilian and industrial sector.

VULNERABILITIES

INTERNET

It is amazingly simple how hackers are able to infiltrate the nation's information infrastructure. One of the most critical portions of the NII is the Internet.



Source: Internet Software Consortium (http://www.isc.org/)

FIGURE 3. INTERNET DOMAIN SURVEY HOST COUNT

The Internet has become the single biggest breakthrough in telecommunications since the telephone. Figure 3 shows the rapid growth in Internet domain hosts from 376,000 in January 1991 to just over 72 million in January 2000.[30]

However, the Internet's growth was spurred on by increased demand without much regard for security. This lack of security measures makes the Internet very vulnerable to attack. The Internet's multiple points of access have yielded multiple points of vulnerability.[31] The Internet as the pipeline for information flow has many vulnerable nodes in which a hacker can penetrate. It is the seamless linkage between telecommunications networks (MCI, Sprint, AT&T, etc.), local networks and Internet service providers that has made the Internet a lucrative target for penetration attempts and could cause significant damage or disruption to the NII. It is this vulnerability that has the United States concerned, as we become increasingly dependent on the Internet for communications.[32] Unlike physical attacks to infrastructure, a cyberattack against a site in Washington D.C. could be conducted from anywhere in the

world through the Internet. It is this difficulty to adequately trace these attacks that has the government and private sector concerned about the protection of the NII.

There are several means in which a cyberattack can achieve its desired effect. Viruses, network worms, Trojan horses, logic bombs and other types of automated attack could disrupt the operations of thousands. There have been several examples of these types of attacks on the NII.

VIRUSES

A hacker can infiltrate the NII by producing a virus throughout the system. Viruses represent the number one cause for shutting down networks and computer systems. In one year, 64 percent of companies around the world were hit by at least one virus.[33] The biggest two viruses to hit the streets were Melissa and Worm. Riding the Internet, these viruses affected e-mail systems, clogged networks and in some cases destroyed data worldwide.[34] Without adequate antivirus software, computers and networks had to be reconfigured or even shut down for days and even weeks until they were repaired.

UNAUTHORIZED NETWORK ENTRY

One of the easiest ways to infiltrate the NII is through weak password protection. An untrained or careless system administrator who has root access can inadvertently provide the hacker, who would gain access through the use of cracking software, the ability to obtain the unsuspecting system administrator's password. Once in possession of the password, the hacker now has in essence the "keys' to the network. With this unlimited access to the network computers, the hacker now has the ability to create havoc throughout the network. The amount of damage and disruption could be devastating. For example, Greenwich Associates, a financial research and consulting firm, had its network broken into by an intruder using a stolen password. With this password, the intruder, believed to be a former employee, was able to gain network access and delete some of the company's research information.[35] Poorly chosen passwords are the weak link in computer security. To reduce successful hacking and infiltration attempts into computer and network systems, it is critical that private sector and government agencies establish and maintain an aggressive password security program and provide system administrators the proper training and support.

NOT READY FOR PRIMETIME SOFTWARE

Another problem that has been uncovered is buggy, commercial, off the shelf software. In order to compete in the dynamic software market, software-manufacturing companies will ship faulty software to companies and government agencies. They will then provide updates through patches to fix the problems. Unfortunately, this software could easily have a bug that could cause a hole in security. In fact, from August 1999 to February 2000, Microsoft released 47 patches to fix security vulnerabilities to its most secure operating system, Windows NT 4.0.[36] The recent unveiling of Microsoft Windows 2000 Professional is another example of the practice of shipping faulty software. Days after its debut, hackers found a security bug that would enable intruders to access the main Windows operating system root

directory and connect to resources using the Administrator's account and a blank password.[37] This hole could provide the hacker a means to access a company's computer and network system, thereby causing major disruptions to the company's database. These vulnerabilities are just the tip of the iceberg. Now more than ever, the government and private sectors need to take responsibility for the protection of the nation's information infrastructure.

RESPONSIBILITIES

Even the most robust information infrastructure defense will not provide 100 percent protection against cyberattacks. Business, government, military, law enforcement and ultimately the nation's security depend upon a shared information system that can be vulnerable to attack. Unfortunately, all our critical banking, transportation data, electrical grids and 95 percent of DoD's unclassified data traffic travel via relatively open communication lines.[38] A 1994 Joint Commission's Report on Redefining Security warned that if an enemy targeted our nation's unprotected civilian information infrastructure, the economic and military results would be disastrous. According to the new information-operations vision, business, government, law enforcement, and national security are all bound together by their shared information systems.[39] Protecting the nation's information infrastructure must be a team approach involving cooperation between government agencies and the private sector. Because both the government and private industry face the same threats, there must be a shared response. Each has a responsibility to ensure the nation's information infrastructure is protected against cyberattacks.

GOVERNMENT SECURITY STRATEGY

President Clinton has outlined in the 1999 National Security Strategy, the major threats to our nation's information infrastructure.

> We also face threats to critical national infrastructures, which increasingly could take the form of a cyber-attack in addition to physical attack or sabotage, and could originate, from terrorist or criminal groups as well as hostile states....
>
> ...This threat is a mix of traditional and non-traditional intelligence adversaries that have targeted American military, diplomatic, technological, economic and commercial secrets. Some foreign intelligence services are rapidly adopting new technologies and innovative methods to obtain such secrets, including attempts to use the global information infrastructure to gain access to sensitive information via penetration of computer systems and networks. We must be concerned about efforts by non-state actors, including legitimate organizations, both quasi-governmental and private, and illicit international criminal organizations to penetrate and subvert government institutions or critical sectors of our economy.[40]

The military has taken the challenge addressed in the National Security Strategy and outlined its strategy in the National Military Strategy.

> Some state or nonstate actors may resort to asymmetric means to counter the US military. Such means include unconventional or inexpensive approaches that circumvent our strengths, exploit our vulnerabilities, or confront us in ways we cannot match in kind.

> Of special concern are terrorism, the use or threatened use of WMD and information warfare. These three risks in particular have the potential to threaten the US homeland and population directly and to deny us access to critical overseas infrastructure.[41]

PRESIDENTIAL DECISION DIRECTIVE 63 (PDD-63)

On May 22, 1998, the President issued Presidential Decision Directive 63 calling for a national effort to assure the security of the vulnerable and interconnected cyber-based infrastructure. It called for a joint public-private action to protect our critical infrastructures. PDD-63 organized the following Federal Government agencies to meet the growing cyber-based challenge.[42]

> National Coordinator for Security, Critical Infrastructure and Counter-Terrorism at the White House National Security Council (NSC) oversees national policy development and implementation for critical infrastructure protection. The National Coordinator is a member of the Cabinet-level Principals Committee, and advises the President and the National Security Advisor on policy and implementation issues as they relate to our national critical infrastructures. The NSC Senior Director for Critical Infrastructure supports him.[43]
>
> The Critical Infrastructure Assurance Office (CIAO), an interagency office housed at the Commerce Department, supports Plan development with Government Agencies and the private sector. The Office is also responsible for assisting Agencies in identifying their dependencies on critical infrastructures, and coordinating a national education and awareness program, legislative issues, and public affairs.[44]
>
> The National Infrastructure Protection Center (NIPC), an interagency office at the FBI, serves as a threat assessment center focusing on threat warnings, vulnerabilities, and law enforcement. The NIPC includes representatives from the FBI, Department of Defense, United States Secret Service, Intelligence Agencies, and other Government Agencies.[45]

NATIONAL PLAN FOR INFORMATION SYSTEMS PROTECTION

On January 7, 2000, the White House released the plan to identify a means to protect the United States' information infrastructure through improved public/private sector cooperation. This plan came about as a result of the President's Commission Report on Critical Infrastructure Protection, which cited that protection of the nation's critical information infrastructure required a new form of cooperation between the government and the private sector.[46] The President's plan is laden with milestones to achieve a successful partnership to help tighten up the security of our nation's information infrastructure.

PRIVATE SECTOR

Despite the government's efforts, the main burden of protecting the nation's information infrastructure must come from the private sector. The government should only be in a supporting role. The private sector has a major stake in the protection of the nation's information infrastructure. With a great deal of business and financial transactions as well as over 95 percent of DoD's unclassified communications utilizing the NII,[47] it is the responsibility of the private sector to ensure the security of its

networks and computer systems. The private sector must have a robust network and network security program complete with trained systems administrators and a solid antivirus protection program. The private sector has the expertise and capital necessary to improve network and computer security through innovations in commercial systems. However, there are several issues that still must be resolved if the United States is going to have a viable information protection program.

ISSUES

In the areas of diagnosing, detecting, and responding to cyberattack, intrusion detection technologies are still in their infancy. Today, the United States has limited ability to detect or recognize a cyberattack against either government or private sector infrastructures, and even less capability to react. A growing battle will continue between the need for security and user accessibility in corporate and government offices. The question of encryption and growing legal issues will continue to cause much discussion. Further, information sharing will be a huge issue as many private sector entities are reluctant to share information about computer intrusions, fearing adverse press coverage and public reaction. The apparent lack of qualified computer specialists will have a significant impact on the nation's ability to investigate attacks against the NII. These are some of the issues that must be addressed for the United States to achieve a viable protection posture against information warfare attacks against its National Information Infrastructure.

INTRUSION DETECTION

Real-time intrusion detection is a key element in any set of defenses. The United States' ability to detect, in real time, intrusions into our systems and to identify the intruder is currently very limited. An information attack can happen in a matter of seconds and damage can occur in an instant. An automated capability to respond to an intrusion, which can prevent or limit the damage to valuable computer and network systems, is imperative.[48]

SECURITY VS ACCESSIBILITY

Maximum security and easy accessibility are not compatible. There has always been a battle between security and functional users. Consequently, because businesses prefer user-friendly equipment, because of profits or ease of use, system security usually takes second priority. The phenomenal growth of computer on-line services and the Internet, only serves to compound the problem. As a result, computer-related crimes become easier to perpetuate and more difficult to identify, investigate, and prove.[49]

INFORMATION SHARING

The extent of attacks on U.S. corporations is difficult to estimate. In some cases, companies do not even recognize the extent of the losses, in others, they fear the negative publicity. As a result, new procedures needed to be developed to provide a "trusted" forum to assure companies that reporting their

vulnerabilities to government or other private sector agencies would not jeopardize the company's operations or provide an advantage to the company's competitors. Seeing this need, PDD-63 has recommended that the private sector, in cooperation with the Federal Government, establish Information Sharing and Analysis Centers (ISACs), to facilitate public-private information sharing on threats, vulnerabilities, anomalies and intrusions. If properly utilized, ISACs could serve as a means to gather, analyze, sanitize, and disseminate private sector information to both industry and to the FBI's National Infrastructure Protection Center.[50] However, the private sector will ultimately decide whether to participate in ISACs and what form these entities will take.[51]

ENCRYPTION

Increased protection against cyberattack can be achieved through encryption technology. Strong digital-signature based authentication used to provide positive access control is perhaps one of the most powerful tools in protection against cyberattack. Encryption can be applied to desktops, file servers, and across networks to assure the privacy of sensitive government, business, and personal information.[52] Computer Systems Policy Project, a coalition of CEOs representing several U.S. computer companies, estimated that without strong encryption, financial losses as a result of computer security breaches could reach $80 billion by the end of year 2000.[53]

The Public Key Infrastructure (PKI), a system of digital certificates and certificate authorities used to verify and authenticate the validity of each party involved in an Internet transaction has been critical to the widespread use of electronic commerce. However, PKI has limitations like any other security solution. If the key to unlock the encrypted code of the message, commonly called the private key, is lost or compromised, privacy is jeopardized. Private keys, if left unprotected by a careless employee, can be copied and used by unauthorized people.[54] Sound security procedures must be set up to reduce the chances of compromise.

However, the real issue is not the use, but the exportation of encryption technology. While U.S. companies want unlimited export of the 128-bit encryption technology to friendly nations in order to compete in the global market, national security organizations fear that uncontrolled export of strong powerful encryption technology without a decryption feature has the potential to be used by hackers to conceal their illegal operations from law enforcement agencies. There have been several bills introduced in Congress that address certain aspects of the encryption issue. However, most of these legislative proposals largely removes existing export controls on encryption products, and open up the opportunity to promote the widespread availability and use of uncrackable encryption products to anyone regardless of the impact on public safety and national security.[55]

LEGAL

Many of our current laws and regulations have not caught up with the new Information Age paradigm.[56] Current legal, cultural and organizational establishments intended to deal with threats to national security are woefully behind the pace of technological change.

Since cyberspace recognizes no borders, international agreements and laws are necessary. This is critical because many information systems are not only national, but also worldwide. An aggressive domestic and international law enforcement policy could have a deterrent effect on potential adversaries.[57]

Because the threats are borderless, one major implication is that it may be very difficult to attribute a particular computer network attack to a foreign state, and to characterize its intent and motive. Another major implication is that an attacker may not be physically present at the place where the effects of the attack are felt. This will complicate the application of traditional rules of international law that were developed in response to territorial invasions and physical attacks by troops, aircraft, vehicles, vessels and weapons that the victim could see and touch, and whose sponsor was usually readily apparent.

CYBERCOPS

Recent hacker attacks in February 2000 against corporate Web sites such as eBay, E-Trade and others have uncovered a problem that may have long term consequences. There is an apparent lack of computer security experts available to investigate cyberattacks. Lured by private security firms offering $150,000 to $200,000, which in most cases is twice their government paychecks, high-caliber forensic computer experts are leaving law enforcement and government service. The nation only has several hundred of these highly qualified experts to investigate an ever-increasing amount of cyberattacks. The implication is that several cases may not be solved because of lack of qualified personnel and resources. The Clinton administration, in an attempt to solve this problem, is requesting an additional $37 Million to hire and train 159 prosecutors and computer analysts as well as build 10 computer forensic labs around the country.[58] However, this may not be enough to stem the tide.

RECOMMENDATIONS

Despite the government's attempts to counter information warfare through public/private sector cooperation, and common sense security precautions, like virus protection, password security procedures and more network administrator training; there are several ways the United States can start being proactive instead of reactive in its defense against information warfare.

1) Put more teeth in the FBI's efforts to pursue hackers by establishing national and international laws against hackers. To have an adequate information protection program, hackers must perceive there is a realistic threat of arrest and punishment. A strong national law and a worldwide law enforced by the World Court and backed by United Nations' resolutions would help deter hackers who would otherwise conduct their cyberattacks against the United States and other countries. However, in order for these

types of laws to be effective they must be enforced. A law without teeth will not be taken seriously and will not be a viable deterrent.

2) Accomplish a nation-wide test of the information infrastructure vulnerabilities to identify weak areas and establish work around procedures in case of a cyberattack. A test to uncover weak areas in the nation's information infrastructure would enable both government and the private sector to adequately rate their systems and take corrective action to bring their systems up to standards. It would also provide a means to work on some worst case cyberattack scenarios. The challenge will be what to do with private sector industries that either deny permission or fail to meet established security standards. Will they be denied access to the nation's information infrastructure? Will the analysis of their vulnerabilities be protected from unauthorized release?

3) Direct government agencies to bring their information system security status up to established security standards and have their progress monitored by the National Infrastructure Protection Center (NIPC). The federal government needs to set the standard for network and computer security. Their compliance should be graded and carefully monitored by the NIPC. The NIPC acting, as an independent agency should provide a rating on how well the agencies conform to established standards. The challenge will be to ensure that information system security standards are consistently evaluated and updated to reflect new technology.

4) Provide incentives to industry and private sector companies that reach or exceed federal/private sector coordinated network and computer security standards either through tax breaks or "special" incentives. Profits or lower costs motivate industry and private sector agencies. If the government could provide incentives such as tax breaks; private sector companies would be financially motivated to improve their network and computer security programs. Their security standards should be evaluated by the NIPC and if they have met or exceeded those standards, those companies should be "rewarded." The challenge will be to ensure that the incentive program remains viable and does not become overloaded with governmental bureaucratic criteria that could jeopardize the improvement efforts of the private sector network and computer security programs. Also, if the private sector primarily relies on financial incentives as motivation to improve their security programs, what happens if the government decides to change its incentive policy?

5) There must be a cooperative effort between U.S. industry and national security agencies on the exportation of encryption technology. An established standard must be agreed upon between private sector and federal agencies to prevent exporting the most sophisticated encryption technology to other countries. The challenge is to apply the encryption technology in a way to effectively protect our critical infrastructure while at the same time meet the demands of global electronic commerce. There needs to be countermeasures, procedures, and realistic export laws established to deter hackers, from using illegally obtained encryption technology while at the same time fostering secure worldwide e-commerce.

CONCLUSION

In order to accomplish these initiatives, the U.S. government will need to make defense of the nation's information infrastructure a top priority and put money and human resources to tackling this potential "threat." The United States can ill afford to take "Infowar" lightly. The United States is the most technologically capable country in the world. Therefore, the United States is the most vulnerable to information warfare due to its dependence upon critical infrastructures and widespread commitments across the globe. The challenge is to find ways to protect our own information systems in order to protect the integrity of both the military operations and the wider social functions, which depend upon them.
WORD COUNT: 5350

ENDNOTES

[1] William J. Clinton, Defending America's Cyberspace, National Plan for Information Systems Protection, An Invitation to a Dialogue (Washington, D.C.: The White House, January 2000), vi.

[2] Lt. Gen. Kenneth A. Minihan, "Defending the Nation Against Cyber Attack: Information Assurance in the Global Environment," 4 November 1998; available from <http://www.usia.gov/journals/itps/1198/ijpe/pj48min.htm>; Internet; accessed 29 October 1999.

[3] National Security Institute, "NII Security: The Federal Role," 5 June 1995; available from <http://nsi.org/library/Compsec/nii.txt>; Internet; accessed 12 January 2000.

[4] Dr. Martin Libicki, Defending Cyberspace and Other Metaphors (Fort McNair: National Defense University, Institute for National Strategic Studies, Center for Advanced Concepts and Technology, 1997.), 13.

[5] Clinton, Defending America's Cyberspace, National Plan for Information Systems Protection, An Invitation to a Dialogue, 2.

[6] ECommerce, "Business to Business to Consumer, Transaction Enabled Internet Solutions," n.d.; available from <http://www.cplus.net/ecommerce/estats.html>; Internet; accessed 7 February 2000.

[7] Clinton, Defending America's Cyberspace, National Plan for Information Systems Protection, An Invitation to a Dialogue, 6.

[8] Reuters, "CIA: Cyberattacks Aimed at U.S.," 25 June 1998; available from <http://www.cnet.com/news/0-1005-200-330625.html>; Internet; accessed 12 January 2000.

[9] Tom Regan, "Military and C4I Cyber Wars, Wars of the Future... Today," 24 June 1999; available from <http://www.infowar.com/mil_c4i/99/mil_c4I_062999a_j.shtml>; Internet; accessed 9 September 1999.

[10] Rod Stark, "Future Warfare: Information Superiority through Info War," 1999; available from <http://www.infowar.com/mil_c4i/stark/FUTURE_WARFARE-INFORMATION_SUPERIORITY_THROUGH_INFOWAR.htm>; Internet; accessed 9 September 1999.

[11] Clinton, Defending America's Cyberspace, National Plan for Information Systems Protection, An Invitation to a Dialogue, 7.

[12] Richard Power, "Computer Crime and Security Survey," Computer Security Issues & Trends Vol V No 1, (Winter 1999): 9.

[13] Greame Browning, "Infowar," 21 April 1997; available from <http://www.govexec.com/dailyfed/o497/042297b1.htm>; Internet; accessed 12 January 2000.

[14] Alvin Toffler and Heidi Toffler, War and Anti-War: Survival at the Dawn of the 21st Century (New York, N.Y.: Little, Brown and Company, 1993), 150.

[15] Bob Woods, "Federal Anti-cyberterrorism Plan Expected Soon," 7 October 1999; available from <http://www.infowar.com/law/99/law_100799c_jshtml>; Internet; accessed 22 October 1999.

[16] Clinton, Defending America's Cyberspace, National Plan for Information Systems Protection, An Invitation to a Dialogue, 9.

[17] Katherine Peters, "Information Insecurity," April 1999; available from <http://www.psycom.net/iwar1.html>; Internet; accessed 12 January 2000.

[18] Clinton, Defending America's Cyberspace, National Plan for Information Systems Protection, An Invitation to a Dialogue, 9.

[19] Gary A. Hayward and Stewart D. Personick, "Protecting the Infrastructures of the Information Age," 1999; available from <http://www.telcordia.com/newsroom/knowledgebase/exchange/winter1999/w99feature2.htm>; Internet, accessed 14 January 2000.

[20] Ibid.

[21] U.S. General Accounting Office, "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks," 22 May 1996; available from <http://www.fas.org/irp/gao/aim96084.htm>; Internet; accessed 21 September 1999.

[22] Clinton, Defending America's Cyberspace, National Plan for Information Systems Protection, An Invitation to a Dialogue, 1.

[23] Ibid.

[24] Ibid.

[25] U.S. General Accounting Office, "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks." 22 May 1996; available from <http://www.fas.org/irp/gao/aim96084.htm>; Internet; accessed 21 September 1999.

[26] Carnegie Mellon Software Engineering Institute, "CERT/CC Statistics," 1988-1999; available from <http://www.cert.org/stats/cert_stats.html>; Internet; accessed 23 January 2000.

[27] Richard Power, "Computer Crime and Security Survey," Computer Security Issues & Trends Vol V No 1, (Winter 1999): 9.

[28] Bob Woods, "Federal Anti-Cyberterrorism Plan Expected Soon," 7 October 1999; available from <http://www.infowar.com/law/99/law_100799c_jshtml>; Internet; accessed 22 October 1999.

[29] Computer Security Institute, "Computer Security Incidents," 24 September 1998; available from <http://www.itg.uiuc.edu/forums/1998-09-24/tsld005.htm>; Internet; accessed 9 November 1999.

[30] Internet Software Consortium, "Internet Domain Survey Host Count," n.d.; available from <http://www.isc.org/>; Internet; accessed 5 January 2000.

[31] Robert Marsh, Critical Foundations, Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection (Washington D.C.: The White House, October 1997), 17

[32] Marsh, Critical Foundations, Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection, 16

[33] Amy K. Larsen. "Global Security Survey: Virus Attack," 12 July 1999; available from <http://www.informationweek.com/743/security.htm>; Internet; accessed 14 January 2000.

[34] Ibid.

[35] Joseph C. Panettieri, "InformationWeek/Ernst & Young Security Survey: Security," 27 November 1995; available from <http://www.informationweek.com/555/55mtsec.htm>; Internet; accessed 26 February 1999.

[36] Microsoft Technet, "Current Security Bulletins," 22 February 2000; available from <http://www.microsoft.com/technet/security/current.asp>; Internet; accessed 26 February 2000.

[37] Stephane Aubert, "Win2K Pro Exposes System During Installation," 16 February 2000; available from <http://www.ntsecurity.net>; Internet; accessed 25 February 2000.

[38] Neil Munro, "Military and C4I, Inducting Information," 29 March 1999; available from <http://www.infowar.com/mil_c4i/99/mil_c4i_032999c_j.shtml>; Internet; accessed 9 September 1999.

[39] Tom Regan, "Military and C4I Cyber Wars, Wars of the Future... Today," 24 June 1999; available from <http://www.infowar.com/mil_c4i/99/mil_c4i_062999a_j.shtml>; Internet; accessed 9 September 1999.

[40] William J. Clinton, A National Security Strategy for a New Century. (Washington, D.C.: The White House, December 1999), 5-6.

[41] General John M. Shalikashvili, National Military Strategy of the United States of America, Shape, Respond, Prepare Now: A Military Strategy for a New Era (Washington, D.C.: The Pentagon, 1997), 9.

[42] Clinton, Defending America's Cyberspace, National Plan for Information Systems Protection, An Invitation to a Dialogue, 22.

[43] Ibid.

[44] Ibid.

[45] Ibid.

[46] Marsh, Critical Foundations, Protecting America's Infrastructures The Report of the President's Commission on Critical Infrastructure Protection, ix.

[47] Libicki, Defending Cyberspace and Other Metaphors,13.

[48] Dr. David S. Alberts, Defensive Information Warfare (Fort McNair: National Defense University, Institute for National Strategic Studies, Center for Advanced Concepts and Technology, 1996.), 73.

[49] Dr. David L. Carter, "Computer Crime Categories: How Techno-criminals Operate," n.d.; available from <http://nsi.org/Library/Compsec/crimecom.html>; Internet; accessed 29 October 1999.

[50] Clinton, Defending America's Cyberspace, National Plan for Information Systems Protection, An Invitation to a Dialogue, 113.

[51] Ibid., 114.

[52] Minihan, "Defending the Nation Against Cyber Attack: Information Assurance in the Global Environment;" 4 November 1998; available from <http://www.usia.gov/journals/itps/1198/ijpe/pj48min.htm>; Internet; accessed 29 October 1999.

[53] Karen Rodriguez, "Encryption Hit Export Stumbling Block," n.d.; available from <http://www.interactiveage.com/032596/602inter2.htm >; Internet; accessed 7 February 2000.

[54] Kevin Plexico, "The Key to E-government," 21 February 2000, available from <http://www.fcw.com/fcw/articles/2000/0221/tech-plexico-02-21-00.asp>; Internet; accessed 27 February 2000.

[55] Louis J. Freech, "Threats to U.S. National Security," 29 January 1998; available from <http://www.infowar.com/civil_de/civil_022798b.html-ssi>; Internet; accessed 22 October 1999.

[56] Alberts, Defensive Information Warfare, 50.

[57] Gary Wheatley and Robert Hayes, "Information Warfare and Deterrence, How Might IW Attacks on the United States Be Deterred?" December 1996; available from <http://www.dodccrp.org/iwdCh2.htm>; Internet; accessed 28 September 1999.

[58] Edward Iwata and Kevin Johnson, "Computer Crime is Outpacing Cybercops," USA Today, 21 February 2000, sec. 1A, pg. 1.

BIBLIOGRAPHY

Abel, David. "Congress to Pentagon – Beef Up Info Tech Oversight." 13 October 1999. Available from <http://www.infowar.com/mil_c4i/99/mil_c4I_101399a_jshtml>. Internet. Accessed 22 October 1999.

Alberts, David S., Ph.D. "Information Warfare and Deterrence." n.d. Available from <http://www.ndu.edu/inss/books/iwd/appd.html>. Internet. Accessed 28 September 1999

Alberts, David S., Ph.D. Defensive Information Warfare. Fort McNair: National Defense University, Institute for National Strategic Studies, Center for Advanced Concepts and Technology, 1996.

Anderson, Kent. "Intelligence-Based Threat Assessments for Information Networks and Infrastructures." 11 March 1998. Available from <http://www.aracnet.com/~kea/Papers/threat_white_paper.shtml>. Internet. Accessed 28 September 1999.

Angelone, J.P. "Protecting Information for the Warfighter – Enabling Information Dominance on the Battlefield." 7 April 1998. Available from <http://www.disa.mil/line/cismid.html>. Internet. Accessed 14 September 1999.

Arquilla, John J., and David F. Ronfeldt. "Cyberwar and Netwar: New Modes, Old Concepts, of Conflict." 1993. Available from <http://www.rand.org/publications/RRR/RRR.fall95.cyber/cyberwar.html>. Internet. Accessed 21 September 1999.

Aubert, Stephane. "Win2K Pro Exposes System During Installation." 16 February 2000. Available from <http://www.ntsecurity.net>. Internet. Accessed 25 February 2000.

Baard, Erik. "Hacker: I Can Black Out 30 U.S. Electric Utility Grids." 15 October 1999. Available from <http://www.infowar.com/hacker/99/hack_101599a_jshtml>. Internet. Accessed 22 October 1999.

Barnett, Roger W. "Information Operation, Deterrence, and the Use of Force." Spring 1998. Accessed from <http://www.nwc.navy.mil/press/review/1998/spring/art1-sp8.htm>. Internet. Accessed 15 November 1999.

Bridis, Ted, "FBI Shorthanded in Battling Hackers." 7 October 1999. Available from <http://www.infowar.com/hacker/99/hack_100999c_jshtml>. Internet. Accessed 22 October 1999.

Browning, Greame. "Infowar." 21 April 1997. Available from <http://www.govexec.com/dailyfed/o497/042297b1.htm>. Internet. Accessed 12 January 2000.

Buchholz, Douglas D., Lt. General. Information Assurance Legal, Regulatory, Policy and Organization Considerations 3rd Edition. Washington D.C.: The Pentagon, 17 September 1997.

Burns, Robert, "Pentagon Assigns Computer Defense." 7 October 1999. Available from <http://www.infowar.com/mil_c4I_100999d_jshtml>. Internet. Accessed 22 October 1999.

Business Wire. "Malicious Virus Attacks Cost Organizations More Than $12 Billion in 1999." 14 January 2000. Available from <http://www.info-sec.com/viruses/00/viruses_011400a_j.shtml>. Internet. Accessed 23 January 2000.

C4I News. "Military and C4I – Task Force Monitoring Cyber Intrusions Around the Clock." 25 July 1999. Available from <http://www.infowar.com/mil_c4i/99/mil_c4I_082599f_j.shtml>. Internet. Accessed 9 September 1999.

Carnegie Mellon Software Engineering Institute, "CERT/CC Statistics." 1988-1999. Available from <http://www.cert.org/stats/cert_stats.html>. Internet. Accessed 23 January 2000.

Carnegie Mellon Software Engineering Institute. "Chapter 6: A Taxonomy of Computer and Network Attacks." n.d. Available from <http://www.cert.org/research/JHThesis/Chapter6.html>. Internet. Accessed 4 November 1999.

Carnegie Mellon Software Engineering Institute. "Security of the Internet." 1997. Available from <http://www.cert.org/encyc_article/tocencyc.html>. Internet. Accessed 14 January 2000.

Carter, David L. Ph.D. "Computer Crime Categories: How Techno-criminals Operate." n.d. Available from <http://nsi.org/Library/Compsec/crimecom.html>. Internet. Accessed 29 October 1999.

Carver, Curtis A., Major. "Information Warfare: Task Force XXI or Task Force Smith." November 1998. Available from <http://www-cgsc.army.mil/milrev/English/SepNov98/carver.htm>. Internet. Accessed 29 October 1999.

Cavoukian, Ann Ph.D. "Go Beyond Security – Build in Privacy: One Does Not Equal the Other." 16 May 1996. Available from <http://www.eff.org/pub/Privacy/960514_cavoukian_priv-sec.speech>. Internet. Accessed 29 October 1999.

Clinton, William J. "White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63." 22 May 1998. Available from <http://www.usdoj.gov/criminal/cybercrime/white_pr.htm>. Internet. Accessed 13 January 2000.

Clinton, William J. A National Security Strategy for a New Century. Washington, D.C.: The White House, December 1999.

Clinton, William J. Defending America's Cyberspace, National Plan for Information Systems Protection, An Invitation to a Dialogue. Washington, D.C.: The White House, 2000.

Cohen, William S. Report of the Quadrennial Defense Review. Washington D.C.: The Pentagon, May 1997.

Cohen, William S. Transforming Defense, National Security in the 21st Century: Report of the National Defense Panel. Washington D.C.: The Pentagon, December 1997.

Cohen, William S., Janet Reno, Jacob J. Lew and William Daley. "Preserving America's Privacy and Security in the Next Century: A Strategy for America in Cyberspace: A Report to the President of the United States." 16 September 1999. Available from <http://www.pub.whitehouse.gov/uri-res /ISR ?urn:pdi: //oma.eop.gov.us /1999/9/17/1.text.1.html>. Internet. Accessed 21 September 1999.

Computer Security Institute. "Computer Security Incidents." 24 September 1998. Available from <http://www.itg.uiuc.edu/forums/1998-09-24/tsld005.htm>. Internet. Accessed 9 November 1999.

Cramer, Myron L., Ph.D. and Stephen R. Pratt. "Computer Viruses in Electronic Warfare." n.d. Available from <http://www.infowar.com/survey/virus_ew.html>. Internet. Accessed 28 September 1999.

Crypt Newsletter. "Pentagon Mandarins: To Save Face, Nose Must Be Amputated." 2 September 1999. Available from <http://www.soci.niu.edu/~crypt/other/jdripper.htm>. Internet. Accessed 28 September 1999.

Devost, Matthew G. "Political Aspects of Class III Information Warfare: Global Conflict and Terrorism." 18 January 1995. Available from <http://www.mnsinc.com/mdevost/montreal.html>. Internet. Accessed 28 September 1999.

Devost, Matthew G. "The Digital Threat: United States National Security and Computers." n.d. Available from <http://www.msninc.com/mdevost/hackers4.html>. Internet. Accessed 11 January 2000.

Devost, Matthew G. "National Security in the Information Age." May 1995. Available from <http://www.terrorism.com/documents/devostthesis.html>. Internet. Accessed 29 October 1999.

Drogin, Bob. "In Theory, Reality, U.S. Open To Cyber-Attack." 9 October 1999. Available from <http://www.infowar.com/hacker/99/hack_101199a_j.shtml>. Internet. Accessed 22 October 1999.

Dunlap, Charles J. Jr., Colonel. "Sometimes the Dragon Wins." 1996. Available from <http://www.infowar.com/mil_c4i/dragon.html-ssi>. Internet. Accessed 15 November 1999.

ECommerce. "Business to Business to Consumer, Transaction Enabled Internet Solutions." n.d. Available from < http://www.cplus.net/ecommerce/estats.html >. Internet. Accessed 7 February 2000.

Ellis, James, David Fisher, Thomas Longstaff, Linda Pesante, and Richard Pethia. "Report to the President's Commission on Critical Infrastructure Protection." January 1997. Available from <http://www.cert.org/pres_comm/cert.rpcci.body.html>. Internet. Accessed 12 November 1999.

Ellison, Robert J., David A. Fisher, Richard C. Linger, Howard F. Lipson, Thomas A. Longstaff, and Nancy R. Mead. "Protecting Critical Systems in Unbounded Networks." December 1999. Available from <http://interactive.sci.cmu.edu/Columns/Security_Matters/1999/December1999/Security.dec99.htm>. Internet. Accessed 12 January 2000.

Fast, William R., Lt Col. "Knowledge Strategies: Balancing Ends, Ways, and Means in the Information Age." n.d. Available from <http://www.ndu.edu/inss/siws/ch1.html>. Internet. Accessed 29 October 1999.

Fields, Craig I. "Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D)." November 1996. Available from <http://cyptome.org/iwd.htm>. Internet. Accessed 12 January 2000.

Fogleman, Ronald R., General, and Sheila E. Widnall. "Cornerstones of Information Warfare." Available from <http://www.infowar.com/mil_c4i/mil_c4ia.html-ssi>. Internet. Accessed 14 September 1999.

Fogleman, Ronald R., General. "Information Warfare and Deterrence – Appendix C. Fundamentals of Information Warfare: An Airman's View." 16 May 1995. Available from <http://www.ndu.edu/inss/books/iwd/appc.html>. Internet. Accessed 29 October 1999.

Forno, Rick. "The Maginot Line of Information Systems Security." March 1999. Available from <http://www.taoiw.org>. Internet. Accessed 11 November 1999.

Forno, Rick. "Why Crypto-Control Will Fail." 20 August 1999. Available from <http://www.taoiw.org>. Internet. Accessed 11 November 1999.

Fowler Bruce W., and Donald R. Peterson. "Induced Fragility in Information Age Warfare." April 1997. Available from <http://lionhrtpub.com/orms/orms-4-97/warfare.html>. Internet. Accessed 11 November 1999.

Freech, Louis J. "Threats to U.S. National Security." 28 January 1998. Available from <http://www.infowar.com/civil_de/civil_022798b.html-ssi>. Internet. Accessed 22 October 1999.

Freedman, Lawrence. "International Centre for Security Analysis – Information Warfare: Will Battle Ever Be Joined?" 14 October 1996. Available from <http://www.infowar.com/mil_c4i/icsa/icsa1.html-ssi>. Internet. Accessed 14 September 1999.

Gibbons, John H. "Cybernation: The American Infrastructure in the Information Age." n.d. Available from <http://www.whitehouse.gov/WH/EOP/OSTP/html/cyber2.html>. Internet. Accessed 21 September 1999.

Global Internet Project. "Jurisdiction in Cyberspace." September 1999. Available from <http://www.gip.org/gipjuris.htm>. Internet. Accessed 4 November 1999.

Global Internet Project. "The Emergence of a Networked World – Commerce, Society and the Future of the Internet." 1996. Available from <http://www.gip.org/gip2h.htm>. Internet. Accessed 4 November 1999.

Goldstein, Steve. "Braced for Cyberwar." 28 December 1999. Available from <http://www.infowar.com/mil_c4i/99/mil_c4i122899b_j.shtml>. Internet. Accessed 11 January 2000.

Gompert, David C. "Keeping Information Warfare in Perspective." Fall 1995. Available from <http://www.rand.org/publications/RRR/RRR.fall95.cyber/perspective.html>. Internet. Accessed 21 September 1999.

Gray, Matthew. "Measuring the Growth of the Web June 1993 to June 1995." 1995. Available from <http://www.mit.edu/people/mkgray/growth/>. Internet. Accessed 14 September 1999.

Greenberg, Lawrence T., Seymour E. Goodman, and Kevin J. Soo Hoo. Information Warfare and International Law. Fort McNair: National Defense University, Institute for National Strategic Studies, Center for Advanced Concepts and Technology, 1998.

Griffin, Samuel B. Sun Tzu, The Art of War. New York, N.Y.: Oxford University Press, 1963.

Hayward, Gary A., and Stewart D. Personick. "Protecting the Infrastructure of the Information Age." 1999. Available from <http://www.telcordia.com/newsroom/knowledgebase/exchange/ winter1999/ w99Feature2.htm>. Internet. Accessed 14 January 2000.

Hoffman, Lisa. "Pros and Cons of a Cyber War Future." 1999. Available from <http://www.freecitizen.com/shns/shns606.htm>. Internet. Accessed 8 November 1999.

Hughes, Patrick M., Lt General. "Global Threats and Challenges: The Decades Ahead." 28 January 1998. Available from <http://www.infowar.com/civil_de/civil_022798a.html-ssi>. Internet. Accessed 22 October 1999.

Infowar.com Ltd. "Information Operations – Developing an Information Operations Treaty." 1998. Available from <http://www.infowar.com/info_ops/info_ops_030399a_j.shtml>. Internet. Accessed 22 October 1999.

Ingle, Jeff and Teresa Lunt. " Research Challenges in High Confidence Networking." 1 July 1998. Available from <http://www.darpa.mil/ito/research/hcn/problems.html>. Internet. Accessed 6 November 1999.

Internet Software Consortium. "Internet Domain Survey Host Count." n.d. Available from <http://www.isc.org/>. Internet. Accessed 5 January 2000.

Iwata, Edward and Kevin Johnson. "Computer Crime is Outpacing Cybercops." USA Today, 21 February 2000, sec. 1A, pg. 1.

Kane, Pamela. PC Security and Virus Protection Handbook, The Ongoing War Against Information Sabotage. New York N.Y.: M&T Books, 1994.

Kopp, Carlo. "Hardening Your Computing Assets." February 1997. Available from <http://www.infowar.com/class_3/harden.html-ssi>. Internet. Accessed 28 September 1999.

Koprowski, Gene. "Hacking the Power Grid." 4 June 1998. Available from <http://www.wired.com/news/news/technology/story/12746.html>. Internet. Accessed 19 January 2000.

Kulmala, Marko. "A Guide to Information Warfare." 1999. Available from <http://infowar.freeservers.com/iw6.html>. Internet. Accessed 21 September 1999.

Kyl, Jon Senator, John S. Tritak, Michael A. Vatis, and Jack Brock. "Hearing Before the Senate Committee on the Judiciary Subcommittee on Technology, and Government Information on Critical Information Infrastructure Protection: The Threat is Real." 6 October 1999. Available from <http://www.senate.gov/~judiciary/w110699.htm>. Internet. Accessed 17 January 2000.

Landesberg, Martha K. and Laura Mazzarella. "Self-regulation and Privacy Online: A Report to Congress – Federal Trade Commission." July 1999. Available from <http://www.eff.org/pub/Privacy/199907_ftc_online_privacy_report.html>. Internet. Accessed 29 October 1999.

Larsen. Amy K. "Global Security Survey: Virus Attack." 12 July 1999. Available from <http://www.informationweek.com/743/security.htm>. Internet. Accessed 14 January 2000.

Laurenzo, Ron. "Ex CIA Director-Cyberwar, Oil Dependence Threaten U.S." 30 November 1999. Available from <http://www.infowar.com/mil_c4i/99/mil_c4I_113099a_j.shtml>. Internet. Accessed 11 January 2000.

Leffall, J. "Law Enforcement Officials Warn of Computer, Internet Crime." 4 June 1999. Available from <http://www.infowar.com/law/99/law_061299e_j.shtml>. Internet. Accessed 22 October 1999.

Leopold, George. "Networks: DoD's First Line of Defense." 13 October 1997. Available from <http://www.techweb.com/wire/news/1997/10/1013dod.html>. Internet. Accessed 28 September 1999.

Levin, Carl Senator. "Statement of Senator Carl Levin (D-Mich.) Before Senate Permanent Subcommittee on Investigations on DoD's Vulnerability to Information Warfare." 22 May 1996. Available from <http://www.senate.gov/~levin/comsec.html>. Internet. Accessed 28 September 1999.

Libicki, Martin C., Ph.D. "Global Information Security." 5 November 1998. Available from <http://www.jya.com/ml110498.htm>. Internet. Accessed 15 November 1999.

Libicki, Martin C., Ph.D. "Perspectives on Defending Cyberspace." n.d. Available from <http://www.ndu.edu/inss/actpubs/dcom/dcomch01.htm>. Internet. Accessed 11 November 1999.

Libicki, Martin C., Ph.D. Defending Cyberspace and Other Metaphors. Fort McNair: National Defense University, Institute for National Strategic Studies, Center for Advanced Concepts and Technology, 1997.

Libicki, Martin C., Ph.D. What is Information Warfare? Fort McNair: National Defense University, Institute for National Strategic Studies, Center for Advanced Concepts and Technology, 1995.

Libicki, Martin C., Ph.D. "Ghosts in the Machines?" 04 November 1998. Available from <http://www.jya.com/ml110498.htm>. Internet. Accessed 15 November 1999.

Lingerfelt, James A. "Strategic for Countering Threats to Information Technology Assets." November 1998. Available from <http://www.usia.gov/journals/itps/1198/ijpe/pj48.bm.html>. Internet. Accessed 11 January 2000.

Ludlow, Peter. "How Should We Respond to Exploratory Hacking/Cracking/Phreaking?" n.d. Available from <http://semlab2.sbs.sunysb.edu/Users/pludlow/intro2.html>. Internet. Accessed 28 September 1999.

MacMillan, Robert. "Military and C4I – Net Warfare Could Short-Circuit US Infrastructure." 4 June 1999. Available from <http://www.infowar.com/mil_c4i/99/mil_c4i060499a_jshtml>. Internet. Accessed 9 September 1999.

MacNulty, Christine A.R. "Changing Social Values and Their Implications for the Ethics of Information Warfare." 31 July 1996. Available from <http://www.infowar.com/Class-1/class-1b.html-ssi>. Internet. Accessed 12 January 2000.

MacRae, Catherine. "Cybercrime Vs Cyber Terrorism, DoD Official Says U.S. Has Been Victim of Cyber Crimes, Not Terrorism." 1 October 1999. Available from <http://www.infowar.com/mil_c4i/99/mil_c4i100699a_j.shtml>. Internet. Accessed 22 October 1999.

Maharg, Paul Ph.D. "Law in the Information Society." 26 February 1999. Available from <http://www.law.warwick.ac.uk/jilt/99-1/maharg.html>. Internet. Accessed 29 October 1999.

Marsh, Robert. Critical Foundations, Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection. (Washington D.C.: The White House, October 1997).

McIntosh, Neil. "Is Big Brother Watching You?" 15 October 1999. Available from <http://www.infowar.com/class_1/99/class1_101599c_j.shtml>. Internet. Accessed 22 October 1999.

McLendon, James W., Colonel. "Information Warfare: Impacts and Concerns." n.d. Available from <http://www.airpower.maxwell.af.mil/airchonicles/battle.chp7.html>. Internet. Accessed 11 January 2000.

McNamara, Joe. "Something Wicked This Web Comes." 7 January 1997. Available from <http://www.eskimo.com/~joelm/wicked.html>. Internet. Accessed 19 January 2000.

Microsoft Technet. "Current Security Bulletins." 22 February 2000. Available from <http://www.microsoft.com/technet/security/current.asp>. Internet. Accessed 26 February 2000.

Miklaszewski, Jim and Robert Windrem. "Pentagon and Hackers in 'Cyberwar'." 5 March 1999. Available from <http://www.zdnet.com/filters/printerfriendly/0,6061,2220773-2,00.html>. Internet. 28 September 1999.

Miller, John H., Ph.D. "Information Warfare: Issues and Perspectives." March 1995. Available from <http:///www.ndu.edu/inss/siws/ch7.html>. Internet. Accessed 28 September 1999.

Minihan, Kenneth A., Lt. General. "Defending the Nation Against Cyber Attack: Information Assurance in the Global Environment." 4 November 1998. Available from <http:///www.usia.gov/journals/itps/1198/ijpe/pj48min.htm>. Internet. Accessed 28 September 1999.

Minihan, Kenneth A., Lt. General. "Statement to the Senate Government Affairs Committee Hearing on Vulnerabilities of the National Information Infrastructure." 24 June 1998. Available from <http://www.senate.gov/~gov_affairs/62498minihan.htm>. Internet. Accessed 11 November 1999.

Mueller, Mark. "Computer 'Crackers' Set Sights On .Gov for Chaos." 1 August 1999. Available from <http://www.bostonherald.com/bostonherald/nat/hack08011999.htm>. Internet. Accessed 19 January 2000.

Munro, Neil. "Military and C4I, Inducting Information." 29 March 1999. Available from <http://www.info.com/mil_c4i/99/mil_c4i_032999c_j.shtml>. Internet. Accessed 9 September 1999.

Myers, Laura. "Pentagon's Computers Fail Hired Hackers' Test." 17 April 1998. Available from <http://www.seattle-times.com/news/nation-world/html98/hack_041798.html>. Internet. Accessed 28 September 1999.

Myers, Steven L. "Federal Commission Predicts Increasing Threat of Terrorism." 21 September 1999. Available from <http://www.infowar.com/class_3/99/class3_092299a_j.shtml>. Internet. Accessed 6 November 1999.

National Defense University. Institute for National Strategic Studies. 1998 Strategic Assessment, Engaging Power for Peace. Washington, D.C.: National Defense University, 1998.

National Security Institute, "NII Security: The Federal Role." 5 June 1995. Available from <http://nsi.org/library/Compsec/nii.txt>. Internet. Accessed 12 January 2000.

Network Computing. "Anatomy of A Network Intrusion." 15 October 1999. Available from <http://www.infowar.com/hacker/99/hack_101899a_j.shtml>. Internet. Accessed 22 October 1999.

New York Times. "Military and C4I - Defense Computers Wide Open to Infiltration." 31 August 1999. Available from <http://www.infowar.com/mil_c4i/99/mil_c4i_083199a_j.shtml>. Internet. Accessed 9 September 1999.

Noach, David. "Cyber 'Hacktivists' Target Spy Network." 18 October 1999. Available from <http://www.infowar.com/hacker/99/hack_101996_jshtml>. Internet. Accessed 22 October 1999.

O'Harrow, Robert Jr. "Computer Security Proposal is Revised." 22 September 1999. Available from <http://www.infowar.com/class_1/99/class1_092499b_j.shtml>. Internet. Accessed 22 October 1999.

O'Neil, Michael J., and James X. Dempsey. "Critical Infrastructure Protection: Threats to Privacy and Other Civil Liberties and Concerns With Government Mandates on Industry." 18 February 1999. Available from <http://www.cdt.org/policy/terrorism/oneildempseymemo.html>. Internet. Accessed 29 October 1999.

Online Air Force News. "Infocons Alert U.S. To Info Threats." 29 April 1999. Available from http://www.cadre.maxwell.af.mil/warfarestudies/iwac/infocon%20article.html>. Internet. Accessed 21 September 1999.

Overill, Richard E., "Computer Crime – An Historical Survey." 10 September 1998. <http://www.kcl.ac.uk/orgs/icsa/crime.htm>. Internet. Accessed 29 October 1999.

Paige, Emmett Jr. "Ensuring Joint Force Superiority in the Information Age." 30 July 1996. Available from <http://www.defenselink.mil/speeches/1996/di1182.html>. Internet. Accessed 21 September 1999.

Panettieri, Joseph C., "InformationWeek/Ernst & Young Security Survey: Security." 27 November 1995. Available from <http://www.informationweek.com/555/55mtsec.htm>. Internet. Accessed 26 February 1999.

Pasternak, Douglas and Bruce B. Auster. "Terrorism at the Touch of a Keyboard." 13 July 1998. Available from <http://www.usnews.com/usnews/issue/980713/13cybe.htm>. Internet. Accessed 11 November 1999.

Peters, Katherine. "Information Insecurity." April 1999. Available from <http://www.psycom.net/iwar1.html>. Internet. Accessed 12 January 2000.

Plexico, Kevin. "The Key to E-government." 21 February 2000. Available from <http://www.fcw.com/fcw/articles/2000/0221/tech-plexico-02-21-00.asp>. Internet. Accessed 27 February 2000.

Plummer, Anne. "Panel: Asymmetrical Attack Threats Are Difficult To Access." 28 December 1999. Available from <http://www.infowar.com/mil_c4i/99/mil_c4I_122899d_j.shtml>. Internet. Accessed 11 January 2000.

Poulsen, Kevin. "Infowar or Electronic Saber Rattling?" 8 September 1999. Available from <http://www.zdnet.com/zdnn/stories/news/0,4586,2330904,00.html>. Internet. Accessed 9 September 1999.

Power, Richard. "Computer Crime and Security Survey." Computer Security Issues & Trends Vol V No 1, (Winter 1999): 1-16.

RAND Research. "Information Warfare: A Two-Edged Sword." n.d. Available from <http://www.rand.org/publications/RRR/RRR.fall95.cyber/infor_war.html>. Internet. Accessed 21 September 1999.

RAND Research. "That Wild, Wild Cyberspace Frontier." Fall 1995. Available from <http://www.rand.org/publications/RRR/RRR.fall95.cyber/wild.html>. Internet. Accessed 21 September 1999.

Rathmell, Andrew Ph.D. "Cyber-terrorism: The Shape of Future Conflict?" October 1997. Available from <http://www.kcl.ac.uk/orgs/icsa/rusi.htm>. Internet. Accessed 11 November 1999.

Rathmell, Andrew Ph.D., Richard Overill Ph.D., Lorenzo Valeri, and John Gearson Ph.D. "The IW Threat from Sub-State Groups: an Interdisciplinary Approach." 20 June 1997. Available from <http://www.infowar.com/mil_c4i/icsa/icsa3.html-ssi>. Internet. Accessed 11 November 1999.

Regan, Tom. "Military and C4I Cyber Wars, Wars of the Future... Today." 24 June 1999. Available from <http://www.infowar.com/mil_c4i/99/mil_c4I_062999a_j.shtml>. Internet. Accessed 9 September 1999.

Reiter, Luke. "CyberCrime Interviews New Anti-hacker Agency Chiefs." 6 March 1998. Available from <http://www.infowar.com/civil_de/civil031098a_s.html-ssi>. Internet. Accessed 6 November 1999.

Reuters. "Big Brother in Cyberspace?" 20 August 1999. Available from <http://www.pcworld.com/pcwtoday/article/0,1510,12413,00.html>. Internet. Accessed 14 September 1999.

Reuters. "Is Cyberterrorism a Real Threat?" 8 June 1998. Available from <http://news.cnet.com/category/0-10050200-330023.html>. Internet. Accessed 11 January 2000.

Reuters. "CIA: Cyberattacks Aimed at U.S." 25 June 1998. Available from <http://www.cnet.com/news/0-1005-200-330625.html>. Internet. Accessed 12 January 2000.

Rodriguez, Karen. "Encryption Hit Export Stumbling Block." n.d. Available from <http://www.interactiveage.com/032596/602inter2.htm>. Internet. Accessed 7 February 2000.

Round W. Oscar, and Earle L. Rudolph, Jr. "Defining Civil Defense in the Information Age." September 1995. Available from <http://www.ndu.edu/inss/strforum/forum46.html>. Internet. Accessed 15 November 1999.

Schneier, Bruce. "Crypto-gram." 15 January 2000. Available from <http://www.info-sec.com/crypto/00/crypto_011700a_j.shtml>. Internet. Accessed 23 January 2000.

Schuman, Joseph. "Military and C4I, Pentagon – Computer Security." 30 August 1999. Available from <http://www.infowar.com/mil_c4i/99/mil_c4I_083099a_j.shtml. >. Internet. Accessed 9 September 1999.

Schwartau, Winn. "The Ethics of Civil Defense and Info Warfare." 29 June 1999. Available from <http://www.icsa.net/library/research/j.shtml>. Internet. Accessed 11 November 1999.

Schwartau, Winn. Information Warfare, Chaos on the Electronic Superhighway. New York N.Y.: Thunder's Mouth Press, 1994.

Shahar, Yael. "Information Warfare: The Perfect Terrorist Weapon." n.d.. Available from <http://www.ict.org.il/articles/infowar.htm>. Internet. Accessed 28 September 1999.

Shalikashvili, John M., General. Joint Vision 2010. Washington D.C.: The Pentagon, 1997.

Shalikashvili, John M., General. Information Warfare: A Strategy for Peace... The Decisive Edge in War. Washington, D.C.: The Pentagon, 1996.

Shalikashvili, John M., General. National Military Strategy of the United States of America, Shape, Respond, Prepare now: A Military Strategy for a New Era. Washington, D.C.: The Pentagon, 1997.

Shamah, David. "Fighting for Your (Computer's) Life." 19 October 1999. Available from <http://www.infowar.com/hacker/99/hack_101999a_j.shtml>. Internet. Accessed 22 October 1999.

Stark, Rod. "Future Warfare: Information Superiority through Info War." 1999. Available from <http://www.infowar.com/mil_c4i/stark/FUTURE_WARFARE-INFORMATION_SUPERIORITY_ THROUGH_ INFOWAR.htm>. Internet. Accessed 9 September 1999.

Stein George J. "Information Attack: Information Warfare in 2025: A Research Paper Presented to Air Force 2025." August 1996. Available from <http://www.au.af.mil/au/2025/volume3/chap03/v3c3-1.htm>. Internet. Accessed 28 September 1999.

Stuever, Hank. "Geek Vs Renegeek, Getting A Lock on Security at Cyber-Terrorism Seminar." 22 September 1999. Available from <http://www.infowar.com/class_3/99/class3_092299b_j.shtml>. Internet. Accessed 6 November 1999.

Sullivan, Bob. "Military and C4I - Cyberwar? – The U.S. Stands to Lose." 3 June 1999. Available from <http://www.infowar.com/mil_c4i/99/mil_c4I_060399c_j.shtml>. Internet. Accessed 9 September 1999.

Suro, Roberto. "FBI Lagging Behind on Cyber Crime." 11 October 1999. Available from <http://www.infowar.com/law/99/law_101199c_j.shtml>. Internet. Accessed 22 October 1999.

Tech Web. "Cyberattacks Against U.S. Are a Matter of Time." 9 October 1999. Available from <http://www.infowar.com/mil_c4i/99/mil_c4I_100999c_j.shtml>. Internet. Accessed 22 October 1999.

Thayer, Rodney. "Network Security: Locking In to Policy." 21 March 1998. Available from <http://www.data.com/tutorials/locking.html>. Internet. Accessed 17 January 2000.

The Center for Democracy and Technology. "DOJ Proposes Secret Searches." 20 August 1999. Available from <http://www.infowar.com/class_1/99/class1_082399b_j.shtml>. Internet. Accessed 22 October 1999.

The Journal of Instructional Warfare and the Centre for Infrastructual Warfare Studies. "1997-1998 Infrastructure Vulnerability Report." September 1998. Available from <http://www.iwar.org/Vul.html>. Internet. Accessed 12 January 2000.

Thom, Greg. "Web of Fear – Cyber Terror May Be the Price We Pay for the Growth of the Internet." 24 July 1999. Available from <http://www.infowar.com/class_3/99/class3_080299a_j.shtml>. Internet. Accessed 22 October 1999.

Thompson, Robert. "Information Warfare – Part 2." Summer 1996. Available from <http://www.dacs.com/awareness/newsletters/summer96/dod.structure.html>. Internet. Accessed 21 September 1999.

Toffler, Alvin and Heidi Toffler War and Anti-War: Survival at the Dawn of the 21st Century. New York, N.Y.: Little, Brown and Company, 1993.

U.S. Defense Science Board. Task Force on Information Warfare-Defense. Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D), by Duane Andrews. Washington D.C.: U.S. Office of the Under Secretary of Defense for Acquisition and Technology, November 1996.

U.S. Department of Defense Office of General Council. "An Assessment of International Legal Issues in Information Operations." May 1999. Available from <http://www.infowar.com/info_ops/info_ops_061599a_jshtml>. Internet. Accessed 23 January 2000.

U.S. General Accounting Office. "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks." 22 May 1996. Available from <http://www.fas.org/irp/gao/aim96084.htm>. Internet. Accessed 21 September 1999.

U.S. Joint Chiefs of Staff. Information Warfare: A Strategy for Peace...The Decisive Edge in War. Washington D.C.: U.S. Joint Chiefs of Staff, 1996.

Vatis, Michael A. "Statement for the Record of Director, National Infrastructure Protection Center Federal Bureau of Investigation on Melissa Macro Virus Before the House Science Committee on Technology." 15 April 1999. Available from <http://www.FBI.gov/pressrm/congress/congress99/vatis1.htm>. Internet. Accessed 17 January 2000.

Vatis, Michael A. "Statement for the Record of Director, National Infrastructure Protection Center Federal Bureau of Investigation on NIPC Cyberthreat Assessment, October 1999." 6 October 1999. Available from <http://www.FBI.gov/pressrm/congress/congress99/nipc10-6.htm>. Internet. Accessed 17 January 2000.

Verton, Daniel. "DoD Investigating Computer 'Mob Tactics'." 30 June 1999. Available from <http://www.fcw.com/pubs/fcw/1999/0628/web-dtra-6-30-99.html>. Internet. Accessed 9 September 1999.

Ware, Willis H. "The Cyber-posture of the National Information Infrastructure." n.d. Available from <http://www.rand.org/publications/mr/mr976/mr976.html>. Internet. Accessed 28 September 1999.

West-Brown, Moira and James Ellis. "Security Matters-Doesn't It?" September 1998. Available from <http://interactive.sei.cmu.edu/Columns/Security_Matters/1998/September1998/Security.sept98.html>. Internet. Accessed 12 January 2000.

West-Brown, Moira and Klaus-Peter Kossakowski, Internal Infrastructure for Global Security Incident Response (Pittsburgh, PA; Carnegie Mellon University, 4 June 1999), 10-13

West-Brown, Moria and Julia Allen. "From Y2K to Security Improvement: A Critical Transition." September 1999. Available from <http://interactive.sei.cmu.edu/Columns/Security_Matters/1999/September1999/Security.sep99.html>. Internet. Accessed 14 January 2000.

West-Brown, Moria. "Avoiding the Trial-by-Fire Approach to Security Incidents." March 1999. Available from <http://interactive.sei.cmu.edu/Columns/Security_Matters/1999/ March1999/security.mar99.htm>. Internet. Accessed 14 January 2000.

Wheatley, Gary and Robert Hayes. "Information Warfare and Deterrence, How Might IW Attacks on the United States Be Deterred?" December 1996. Available from <http://www.dodccrp.org/iwdCh2.htm>. Internet. Accessed 28 September 1999.

Whine, Michael. "Cyberspace – A New Medium for Communication, Command and Control by Extremists." 5 May 1999. Available from <http://www.ict.org.il/articles/articledet.cfm?articleid=76.html>. Internet. Accessed 28 September 1999.

Wilson, Michael, "Defense in Depth: Design Notes." 1997. Available from <http://www.7pillars.com/papers/didfinal.htm>. Internet. Accessed 11 Nov 1999.

Wilson, Michael. "Hardwar, Softwar, Wetwar Operational Objectives of Information Warfare." 1995. Available from <http://www.fas.org/cp/eprint/96/hswwar.htm>. Internet. Accessed 11 November 1999.

Wilson, Michael. "Infrastructural Warfare Threat Model." 1996. Available from <http://www.7pillars.com/papers/MT.html>. Internet. Accessed 11 Nov 1999.

Wilson, Michael. "National Security and Infrastructual Warfare." 1998. Available from <http://www.7pillars.com/papers/natlsec.html>. Internet. Accessed 11 Nov 1999.

Wilson, Michael. "Terrorism in a New World—Evolution in Revolution." 1994. Available from <http://www.fas.org/cp/eprint/96/terror.htm>. Internet. Accessed 28 September 1999.

Wilson, Michael. "Waging IWAR." 1997. Available from <http://www.7pillars.com/papers/Waging.html>. Internet. Accessed 11 Nov 1999.

Wilson, Peter L. "The Information War." 17 March 1995. Available from <http://www.t0.or.at/hakimbey/infowar.htm>. Internet. Accessed 21 September 1999.

Wolfe, Frank. "Defense Daily - Joint Task Force to Direct Pentagon's Cyber Defense." 26 January 1999. Available from <http://www.cadre.maxwell.af.mil/warfarestudies/iwac/dd26JAN99.html>. Internet. Accessed 21 September 1999.

Wolfe, Jim. "FBI Traces Cyber Raids to Russia." 7 October 1999. Available from <http://www.infowar.com/hacker/99/hack_100799c_j.shtml>. Internet. Accessed 22 October 1999.

Woods, Bob. "Federal Anti-cyberterrorism Plan Expected Soon." 7 October 1999. Available from <http://www.infowar.com/law/99/law_100799c_jshtml>. Internet. Accessed 22 October 1999.

XINHUA. "Pentagon Officials Warn of Electronic Pearl Harbor." 11 March 99. Available from <http://www.infowar.com/mil_c4i/99/mil_c4I_031199c_j.shtml>. Internet. Accessed 9 September 1999.

Zakon, Robert H. "Hobbes' Internet Timeline v4.2." 1999. Available from <http://info.isoc.org/guest/zakon/Internet/History/HIT.html>. Internet. Accessed 14 September 1999.